Published on *The National Law Review* https://natlawreview.com

New Cyber Security Rules for US Technology Companies Operating in the EU

Article By:

Caroline Churchill

Andrew Kimble

The EU is in the course of passing a range of new cyber security legislation which will apply to US businesses who provide services in the EU. One part of that legislative programme is the new Network and Information Security Directive (called '**NIS2**') which is designed to protect the critical infrastructure of the EU and which imposes personal liability on board members who fail to protect that infrastructure from cyber attacks.

The original Network and Information Security Directive ("**NIS1**") was originally passed back in 2016. It focused on protecting physical infrastructure like water pipes and power lines by requiring the suppliers of those services (both private businesses and public entities) to have appropriate cyber security measures in place.

Eight years later, digital infrastructure is now vital to the functioning of the EU economy so NIS2 expands the scope of the security requirements to many different types of technology services, which will draw more US businesses under the regulations. NIS2 applies to both businesses based in the EU and also to some business based outside the EU but which supply services into the EU. In particular, NIS2 applies to various different types of US technology companies, including:

- Cloud computing service providers
- Data centre service providers
- Content delivery network providers
- Managed service providers
- Managed security service providers
- Search engines
- Online market places
- Social network platforms

If NIS2 applies to your business, then you will be required to have in place appropriate cyber security controls to protect your operations from any significant disruption. The headline obligations under NIS2 are as follows:

- There are 10 required cyber security measures that must be in place.
- Your management team must oversee your cyber security and be trained on cyber security.
- If you suffer a significant disruption in your operations caused by an IT failure (whether or not caused by a cyber-attack), you will need to notify the regulator within 24 hours and possibly also your customers.
- Failure to comply can lead to penalties of up to €10m or 2% of global turnover (whichever is higher).
- Your management team may also have personal liability.

NIS2 was supposed to be in force from 17 October 2024, but many EU states have failed to implement it on time. As an EU Directive, member states are required to implement NIS2 and so NIS2 laws are expected to start to apply across the EU during late 2024 / early 2025. There is therefore a window now in which to ensure compliance with the new rules.

NIS2 is only part of a suite of cyber security laws in the EU that have extra-territorial effect and can apply to US businesses. The General Data Protection Regulation already requires organisations to implement appropriate security measures to protect personal data. In January 2025, the Digital Operational Resilience Act ("**DORA**") comes into force. It places stringent and prescriptive obligations on EU financial institutions to ensure the continuity of their IT systems and mandates them to risk-assess, monitor and put in place contract terms with their suppliers. US businesses supplying services in the EU financial services sector will feel the effects of DORA flowed down to them by their customers. Finally, the EU has recently passed the Cyber Resilience Act which will directly apply to many US software and hardware companies, in some cases mandating them to have their products assessed by third-party testing houses to certify that they are secure. Further client alerts on these new developments will follow in the coming weeks.

National Law Review, Volume XIV, Number 313